**Riesgo:**

En el momento de admisión de un paciente se interrumpe el acceso al sistema sanatorial por problemas de conexión en la red LAN de la organización,  lo que impide el continuar con el proceso de admisión de pacientes

**INVENTARIO DE ACTIVOS**

**Escalas de valores:**

1. Muy bajo, 2. Bajo, 3. Medio, 4. Alto, 5. Muy alto

| **ID** | **ACTIVO** | **TIPO** | **CONTENEDOR** | **RELACIONADOS** | **DUEÑO** | **CUSTODIO** | **C** | **I** | **D** | **Crit.** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | Proceso de Atención Ambulatoria | Proceso |  |  | Jefe de Atenciones Ambulatorias | Empleados de Atención Ambulatoria  Enfermeras  Médicos de Atención Ambulatoria | 5 | 5 | 5 | 15 |
| 2 | Red LAN | Hardware | Instalaciones del Departamento de Sistemas y de los usuarios en sus puestos de trabajo | 3,4.5 | Jefa de Sistemas | Personal de Sistemas | 3 | 5 | 5 | 13 |
| 3 | Servidor | Hardware | Instalaciones del Departamento de Sistemas | 2,1,5 | Jefa de Sistemas | Personal de Sistemas | 4 | 5 | 5 | 14 |
| 4 | Pc de los usuarios | Hardware | Instalaciones del Sanatorio |  | Jefe de Sector | Usuarios del Sistema Sanatorial y Personal de Sistemas | 3 | 3 | 5 | 11 |
| 5 | Sistema sanatorial | Software | Servidor, PC de los usuarios | 4,3,1 | Jefa de Sistemas | Personal de Sistemas, Usuarios del Sistema Sanatorial | 5 | 5 | 5 | 15 |
|  |  |  |  |  |  |  |  |  |  |  |

**IDENTIFICACIÓN DE RIESGOS**

| **Id.** 01 |  | | | |
| --- | --- | --- | --- | --- |
| **Identificador** | **Legajo:** | **Apellido y Nombres:** | | |
| **Especificación** | En el momento de admisión de un paciente se interrumpe el acceso al sistema sanatorial por problemas de conexión en la red LAN de la organización,  lo que impide el continuar con el proceso de admisión de pacientes. | | | |
| **Clasificación** | **Fallas de Sistemas y Tecnología** | | **Hardware** | **Mantenimiento/Obsolescencia.** |
| **Contexto** | | | | |
| **Descripción** | El desarrollo del proceso requiere la interacción constante con el sistema sanatorial. Los datos registrados en la base de datos del sistema son requeridos en cada interacción, ya sea en la admisión (el caso particular de este riesgo) donde no se podrá corroborar el turno del paciente ni registrar su asistencia, como tampoco los datos requeridos para su atención.  Todos los usuarios de la organización están conectados a la red LAN de la organización. Una falla en la misma deja a los usuarios sin la **disponibilidad** del sistema sanatorial.  Si la falla se produce (como dice el riesgo) en el momento de mayor afluencia de público el impacto en el proceso será catastrófico.  Los usuarios están capacitados para requerir los datos que se requieren para la atención (que podrá realizarse en forma manual).  Se deberá revisar si el problema de conexión está relacionado con:   * Desconexión de la PC de la Red (de un usuario de admisión en particular) * Fallas en el equipo de red * Rotura de algún componente * Fallas en la configuración. | | | |
| **Valoración del Riesgo** | | | | |
| **Factores para evaluar la magnitud de pérdida**  **Activos**: En la planilla de activos se ha establecido el nivel de criticidad de los activos afectados. Además, se pueden considerar:   * **Productividad**: La imposibilidad de utilizar el sistema (por falla en la red) para las atenciones ambulatorias pueden repercutir en el flujo del proceso y generará un impacto en la productividad. * **Costo de reemplazo**: Este costo estará dado por: la detección de la falla en la red, su reparación (el tiempo del personal de sistemas encargado de reparar la red), el costo de los elementos para repararlo, el tiempo que el sistema estará parado y el flujo de personas que requirieron atención manual mientras el sistema está caído lo que determinará el tiempo que se requiere para reprocesar la información que no haya quedado en el sistema por la falla. Esta información se deberá volcar al sistema una vez solucionada la falla. * **Sensibilidad**: En este riesgo no se trata la divulgación o uso indebido de información confidencial.   + **Reputación:** No aplica   + **Ventaja competitiva**: No aplica   + **Legal / Regulatoria:** No aplica   + **General**: No aplica * **Volumen:** En este caso el volumen estará dado por:   + cantidad de pacientes que se han presentado a partir de la materialización del riesgo y todos los datos de la atención han debido registrarse en forma manual.   **Amenazas:**  El estado de las redes constituye una amenaza.   * **Competencia:** El conocimiento del estado de las redes de la organización es responsabilidad de la Jefa de Sistemas y del Personal del área de sistemas * **Internas/Externas:** es una amenaza interna por lo que se debería tener control total sobre la misma. * **Acción:**   + **Acceso**: No aplica   + **Uso indebido**: No aplica   + **Divulgación**: No aplica   + **Modificación**: No aplica   + **Denegación de acceso**: lo que sucede es la denegación de acceso al servidor de la organización (relacionada con los activos de información)   **Organización:** El riesgo existe dentro del contexto del sanatorio y el riesgo ocasiona la pérdida de la capacidad de operar normalmente   * **Momento**: La atención sanatorial es continua por lo que una falta de conexión tendrá un impacto de pérdida alto sobre todo en los momentos de mayor afluencia de público. * **Debido cuidado:** No se conocen medidas preventivas (indicadas en el contexto del riesgo) para mitigar esta amenaza por lo que se deberán considerar en las estrategias de tratamiento de este. * **Detección:** La detección se dará en el momento en que se produzca la materialización del riesgo, ya sea por un monitoreo por parte del Personal del área de Sistemas o por un aviso de los usuarios del sistema a los que se les ha denegado el acceso. * **Respuesta:** No se especifica en el riesgo si la organización está preparada para operar ante la materialización del riesgo. En función de esto se puede analizar:   + **Contención**: El personal está capacitado para conocer los requerimientos de información del proceso (podría actuar ante la materialización).   + **Remediación**: Se podrá revisar la posibilidad de reparar/configurar la red de la organización   + **Recuperación**: Una vez establecida la conexión el sistema sanatorial estará disponible. La información que haya sido trabajada en forma manual a partir de la materialización del riesgo deberá ser registrada en el sistema.   **Factores externos:** Este puede ser un riesgo que pueda ser utilizado por entidades externas para aumentar el impacto de la pérdida   * **Detección:** No aplica. * **Legal / Regulatorio**: No aplica. * **Competidores**: Los competidores pueden utilizar esta información para bajar la imagen de la organización (bajo). * **Medios de comunicación**: Idem competidores. * **Otros grupos de interés:** No aplica   **Utilizando la escala de valores se puede decir que el impacto es: Muy Alto (5).**  **Factores utilizados para el cálculo de la probabilidad:**  **Frecuencia de amenazas**:   * **Contacto**: El uso de las redes de la organización es intensivo   **Aleatorio: -- Regular**: **X** **Intencional**: **--**   * **Acción**: Materializado el riesgo el proceso se ve afectado en su operatoria normal.   + **Beneficio**: No existe beneficio   + **Nivel de esfuerzo**: No existe nivel de esfuerzo si las redes no tienen mantenimiento o son obsoletas   + **Riesgo de detección**: es fácilmente detectable la falta de conexión   **Vulnerabilidades**: Deben evaluarse estrategias para resistir las acciones del agente de amenaza, trabajando sobre el activo en sí y sobre los activos que afecta la materialización del riesgo.   * **Capacidad de las amenazas**: El nivel probable de fuerza de la desconexión de red (agente de amenaza) sobre el proceso (activo) es muy alto ya que se depende de la misma para poder operar. La falta de controles en caso de la red física en sí, o de capacitación a los usuarios en el caso de que la desconexión sea específicamente de la PC del usuario, son las capacidades que están en juego para la materialización del riesgo. * **Capacidad de resistencia** (CR): Los empleados administrativos que operan en la atención están altamente capacitados para requerir al paciente toda la información que se necesita para cada tipo de atención ambulatoria (capacidad de resistencia) por lo que solicitarán al paciente dicha información, pero la misma no quedará registrada en el sistema para continuar con el proceso, como tampoco la información de las restantes actividades del proceso.   **Utilizando la escala de valores se puede decir que la probabilidad es: Alta (4).** | | | | |
| **Consecuencias** | Toda información que se requiera del sistema, en la que los datos que no han podido registrarse deban ser analizados, no podrá obtenerse hasta tanto se recupere el proceso una vez materializado el riesgo. | | | |
|  |  |  |  |  |

**TRATAMIENTO DE RIESGOS**

| **Id.** 01 | |  | |
| --- | --- | --- | --- |
| **Identificador** | | **Legajo:** | **Apellido y Nombres:** |
| **Especificación** | | En el momento de admisión de un paciente se interrumpe el acceso al sistema sanatorial por problemas de conexión en la red LAN de la organización, lo que impide el continuar con el proceso de admisión de pacientes | |
| **E S T A T E G I A S** | **Evitar** | | |
| Se puede evitar la materialización del riesgo utilizando otro tipo de infraestructura para la operación de los sistemas del Sanatorio | | |
| **Transferir** | | |
| 1. Utilizar servicios en la Nube como infraestructura de los sistemas del Sanatorio y que la conexión sea a través de internet. Especificar SLA para acordar el servicio. | | |
| **Mitigar** | | |
| En cuanto a mitigar la probabilidad de materialización del riesgo:   1. Aumentar la detección temprana de la posible materialización del riesgo: Realizar controles y seguimientos periódicos del estado de la red interna de la organización. Realizar recambios de componentes considerando el período de obsolescencia programado. Esta actividad es interna a la organización ya que el personal del área de sistemas es el que se encarga del soporte técnico de la infraestructura. 2. Para los casos donde un problema de conexión afecte a un usuario en particular de la sección de admisión: Tener una PC alternativa en el sector conectada al sistema para uso en caso de este tipo de fallas.   En cuanto a mitigar el impacto de la materialización del riesgo:   1. Especificar procedimiento manual para las actividades afectadas (continuidad del negocio):    1. Especificar el procedimiento para dejar asentados manualmente todas las admisiones nuevas armando un legajo que será luego transferido a cada sector correspondiente y deberá ser devuelto al área de admisión para el registro posterior una vez recuperada la conexión    2. Capacitar a los empleados que intervienen en el proceso en la operatoria manual y en el reproceso de los datos (sobre el uso y salvaguarda de los datos)    3. Especificar el procedimiento para el vuelco de la información manual al sistema una vez recuperada la conexión 2. Utilizar una infraestructura de respaldo (relacionada con la estrategia de transferencia Item 1)    1. Especificar el procedimiento del área de sistemas para intercambiar la operación entre la red LAN y la red por internet con conexión a los servicios en la nube.    2. Especificar el procedimiento para volcar los registros que hayan sido subidos a la infraestructura en la nube una vez recuperada la conexión a la red de la organización | | |
| **C O N**  **T**  **R**  **O**  **L**  **E**  **S** | Los controles que garantizan las estrategias de mitigación/transferencia mencionadas son:  Estrategia 1 (mitigación):   * Seguridad Física y ambiental   + Seguridad de los equipos.     - Mantenimiento de los equipos   Evidencias objetivas: Especificación de la infraestructura. Informes de revisión de la infraestructura.  Estrategia 4 (mitigación) y 1(transferencia):   * Relaciones con suministradores   + Gestión de la prestación del servicio por suministradores.     - Supervisión y revisión de los servicios prestados por terceros.   Evidencias objetivas: SLA en relación a la provisión del servicio en la nube. Pago del servicio en tiempo y forma.  Estrategia 3 (mitigación):   * Aspectos de la Seguridad de la información en la gestión de la continuidad de Negocio   + Continuidad de la seguridad de la información.     - Planificación de la continuidad de la seguridad de la información.   Evidencias objetivas: Análisis de tratamiento de la información y especificación de procedimientos en caso de fallas en los sistemas específicos   * Seguridad en la operativa   + Responsabilidades y procedimientos de operación.     - Documentación de procedimientos de operación.   Evidencias objetivas: Documentación del procedimiento y definición de responsabilidades   * Seguridad ligada a los recursos humanos   + Durante la contratación     - Concientización, educación y capacitación en seguridad de la información   Evidencias objetivas: planes de capacitación, informe de asistencia a capacitaciones, evaluaciones de desempeño | | |
| **Riesgo Residual** | | | |
| Se puede analizar que:  La probabilidad se puede ver disminuida en función de aplicar las estrategias 1,2 y 4 de mitigación y 1 de transferencia  El impacto se puede disminuir aplicando las estrategias 3 y 4 de mitigación y 1 de transferencia.  Se puede decir que se baja la severidad del riesgo, el impacto a medio y la probabilidad a bajo. | | | |
|  |  |  |  |

**PLANES DE CONTINGENCIA, RECUPERACIÓN Y CONTINUIDAD DE NEGOCIO**

| **Id.** 01 |  | |
| --- | --- | --- |
| **Identificador** | **Legajo:** | **Apellido y Nombres:** |
| **Especificación** | En el momento de admisión de un paciente se interrumpe el acceso al sistema sanatorial por problemas de conexión en la red LAN de la organización, lo que impide el continuar con el proceso de admisión de pacientes | |
| **Disparadores** | 1. Personal del área de Sistema que monitorea los estados de la infraestructura detecta la falta de conexión 2. Falta de conexión detectada por el usuario, ya que el sistema acusa el error en el momento de acceso a los datos. | |
| **Contingencia** | En caso de falla de conexión detectada:   1. Se registra el incidente (detectado por el personal que realiza el control de la infraestructura o por un usuario). 2. Personal de sistema monitoriza la infraestructura.   En caso de una falla en la PC de un usuario y la infraestructura de red funciona correctamente:   1. Se solicita al usuario que revise la conexión de su PC 2. Si el usuario no puede solucionarlo, personal de sistemas se encarga de su solución y se repara (Fin).   En caso de una falla en la infraestructura de RED y se cuenta con infraestructura alternativa en la nube:   1. El personal de sistema ejecuta el procedimiento para el cambio de operación. 2. Se avisa al personal que se realizará el cambio a operación a la infraestructura alternativa hasta tanto se recupere indicando el tiempo estimado   En caso de una falla en la infraestructura de RED y NO se cuenta con infraestructura alternativa en la nube:   1. Se avisa al personal que deberá trabajar en forma manual hasta tanto se recupere la conexión indicando el tiempo estimado | |
| **Recuperación** | En caso de una falla en la PC de un usuario y la infraestructura de red funciona correctamente:   1. No requiere recuperación. El usuario continuo trabajando en el otro equipo (ver continuidad de negocio)   En caso de una falla en la infraestructura de RED y se cuenta con infraestructura alternativa en la nube:   1. Se analiza el momento de recuperación para que el mismo no afecte a muchos usuarios. 2. Se avisa al personal que quedará sin conexión por un tiempo para generar el cambio de operación. 3. Se vuelca la información procesada en la nube al sistema de la organización. 4. Se avisa a los usuarios que el sistema ha sido recuperado.   En caso de una falla en la infraestructura de RED y NO se cuenta con infraestructura alternativa en la nube:   1. Se avisa al personal que deberá trabajar en forma manual hasta tanto se recupere la conexión indicando el tiempo estimado 2. Para la recuperación de los ingresos de los cuales no se hayan registrado los datos se seguirá el procedimiento especificado en la estrategia de mitigación 3, item c. 3. El sistema fue recuperado correctamente   En cualquier caso documentar el tratamiento del incidente | |
| **Continuidad de Negocio** | En caso de una falla en la PC de un usuario y la infraestructura de red funciona correctamente:   1. El usuario continúa trabajando en el equipo alternativo disponible en el área de admisión   En caso de una falla en la infraestructura de RED y se cuenta con infraestructura alternativa en la nube:   1. Los usuarios continúan trabajando normalmente utilizando el sistema alternativo en la nube.   En caso de una falla en la infraestructura de RED y NO se cuenta con infraestructura alternativa en la nube:   1. Se utiliza el procedimiento de registro manual identificado en la estrategia de mitigación 3. Item a. | |
| **Controles de Garantía de los Planes** | Los controles que garantizan la ejecución de planes de contingencia, recuperación y continuidad de Negocios mencionadas son:   * Aspectos de la Seguridad de la información en la gestión de la continuidad de Negocio   + Continuidad de la seguridad de la información.     - Verificación, revisión y evaluación de la continuidad de la seguridad de la información.   Evidencias Objetivas: Informes de simulacros de materialización del riesgo   * Gestión de Incidentes en la seguridad de la información.   + Gestión de incidentes de seguridad de la información y mejoras.   + Responsabilidades y procedimientos.   + Notificación de los eventos de seguridad de la información.   + Notificación de puntos débiles de la seguridad.   + Valoración de eventos de seguridad de la información y toma de   + decisiones.   + Respuesta a los incidentes de seguridad.   + Aprendizaje de los incidentes de seguridad de la información.   + Recopilación de evidencias.   Evidencias objetivas: SLA, Documentación de la materialización del riesgo, documentación de los procedimientos de Contingencia, Recuperación y Continuidad de Negocio   * Relaciones con suministradores   + Gestión de la prestación del servicio por suministradores.     - Supervisión y revisión de los servicios prestados por terceros.   Evidencias Objetivas: Informe de incumplimiento del SLA acordado para el servicio en la nube. | |